CLAIMS:

1. Method for secure data communication between consumer devices, the method comprising the following steps:

a) activating a data communication link between the devices,

b) transmitting data between the devices for performing an authentication session (3) for authenticating the consumer devices (1,2), wherein the authentication session (3) generates a first key (5), characterized in that the method further comprises the step of:

c) transmitting data between the devices for performing another authentication session (4) for authenticating the consumer devices (1,2), wherein the authentication session (4) generates a second key (6).

2. The method as claimed in claim 1, characterized in that the method further comprises the step of:

d) generating a link key (9) for encrypting and/or decrypting the data communicated over the data communication link by merging the first key (5) with the second key (6) using a key merge function.

3. The method as claimed in claim 1 or 2, characterized in that the authentication sessions are performed independent of each other.

4. The method as claimed in claim 1, characterized in that step b) further comprises transmitting additional data between the devices for deciding whether of not to proceed with step c).

5. The method as claimed in claim 1, characterized in that the first authentication session is an authentication session as described in the Bluetooth link encryption specification.

6. The method as claimed in claim 2, characterized in that the key merge function has one or more of the following properties:

- for any two given first and second keys as input in the key merge function, the link key output of the key merge function is uniquely specified;

- the number of link key output bits is constant; - if the second key is undefined or all zero, the link key output bits are identical to the bits of the first key;

- for any first key, the uncertainty in the output is approximately equal to the uncertainty of the second key;

- for any second key, the uncertainty in the output is approximately equal to the uncertainty of the first key.

7. The method as claimed in claim 6, characterized in that the key merge function is a bit-wise XOR-function.

8. The method as claimed in claim 2, characterized in that the key merge function comprises encrypting the first key with the second key or vice versa.

9. Consumer device for performing the method according to one of the claims 1 to 8, the consumer device comprising means for activating a data communication link, means for transmitting data, authentication means for performing an authentication session and further authentication means for performing another authentication session.

10. The consumer device as claimed in claim 9, characterized in that the consumer device further comprises an Application Programmers Interface (API) for informing the consumer device about the protection status of another consumer device.

11. The consumer device as claimed in claim 9 or 10, characterized in that the consumer device further comprises receiving means for receiving information, decrypting means for decrypting the information using the link key (9) and recording means for recording the information.

12. The consumer device as claimed in claim 9, wherein the consumer device is a portable device, e.g. a headphone or a walkman.

13. The consumer device as claimed in claim 9, wherein the consumer device comprises means for performing short-range wireless data communication.

14. Signal comprising data transmitted between the devices (1,2) as used in any one of the methods 1 to 9, wherein the data is used for performing the authentication sessions (3,4) for authenticating the devices.

15. Signal comprising a first key (5) and a second key (6) obtained after performing the method of any one of the methods 1 to 9.

16. Signal according to claim 15, characterized in that it further comprises a link key (9) for encrypting and/or decrypting the data communicated over the data communication link, the link key being generated by merging the first key (5) with the second key (6) using a key merge function.